

Audit Report



DEFENSE INFORMATION SYSTEMS AGENCY
MANAGEMENT OF MAINFRAMES

Report No. 99-182

June 9, 1999

Office of the Inspector General
Department of Defense

DTIC QUALITY INSPECTED 4

DISTRIBUTION STATEMENT A
Approved for Public Release
Distribution Unlimited

19990806 052

AQI 99-11-1973

Additional Copies

To obtain additional copies of this audit report, contact the Secondary Reports Distribution Unit of the Audit Followup and Technical Support Directorate at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932 or visit the Inspector General, DoD, Home Page at: www.dodig.osd.mil.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact the Audit Followup and Technical Support Directorate at (703) 604-8940 (DSN 664-8940) or fax (703) 604-8932. Ideas and requests can also be mailed to:

OAIG-AUD (ATTN: AFTS Audit Suggestions)
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-2884

Defense Hotline

To report fraud, waste, or abuse, contact the Defense Hotline by calling (800) 424-9098; by sending an electronic message to Hotline@dodig.osd.mil; or by writing to the Defense Hotline, The Pentagon, Washington, D.C. 20301-1900. The identity of each writer and caller is fully protected.

Acronyms

DISA	Defense Information Systems Agency
DISA WESTHEM	DISA Western Hemisphere
CDAs	Central Design Activities
Y2K	Year 2000



INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-2884

June 9, 1999

MEMORANDUM FOR ASSISTANT SECRETARY OF DEFENSE (COMMAND,
CONTROL, COMMUNICATIONS, AND
INTELLIGENCE)

SUBJECT: Defense Information Systems Agency Management of Mainframes
(Report No. 99-182)

We are providing this audit report for your information and use. Management comments on a draft were considered in preparing the final report.

Comments on the draft of this report conformed to the requirements of DoD Directive 7650.3 and left no unresolved issues. Therefore, no additional information is required.

We appreciate the courtesies extended to our staff. For additional information on this report, please contact Mr. Kenneth H. Stavenjord at (703) 604-8952 (DSN 664-8952) (kstavenjord@dodig.osd.mil) or Ms. Mary Lu Ugone at (703) 604-9049 (DSN 664-9049) (mlugone@dodig.osd.mil). See Appendix B for the report distribution. Audit team members are listed on the inside of the back cover.

A handwritten signature in black ink, reading "Robert J. Lieberman", is positioned above the typed name.

Robert J. Lieberman
Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. 99-182
(Project No. 9AS-0092)

June 9, 1999

Defense Information Systems Agency Management of Mainframes

Executive Summary

Introduction. The National Defense Authorization Act for FY 1999 requires the Inspector General, DoD, to selectively audit information technology and national security systems certified as year 2000 compliant to evaluate their ability to successfully operate in the year 2000, including their ability to access and transmit information from point of origin to point of termination. This is one in a series of reports addressing that requirement. In addition, this is also one in a larger series of reports being issued by the Inspector General, DoD, in accordance with an informal partnership with the Chief Information Officer, DoD, to monitor DoD efforts to address the year 2000 computing challenge. For a listing of audit projects addressing the issue, see the year 2000 webpage on the IGnet at <http://www.ignet.gov>.

Objectives. The overall evaluation objective was to follow up on Inspector General, DoD, Report No. 98-193, "Evaluation of the Defense Megacenters Year 2000 Program," August 25, 1998. Specifically, we evaluated whether the Defense Information Systems Agency is adequately managing the mainframe domains, in coordination with the Central Design Activities and functional users, to ensure mainframe domain year 2000 compliance.

Evaluation Results. The Defense Information Systems Agency and the Central Design Activities have made significant progress in identifying and renovating the domains at the Defense Megacenters; however, additional work is needed to lower the risk of year 2000 date-related failures. As of March 31, 1999, the Defense Information Systems Agency still had 94 domains identified as noncompliant. Forty percent of the noncompliant domains are shared between and among Military Departments and Defense Agencies, causing risks to applications that reside on the shared noncompliant domains. See the finding section for details on the evaluation results.

Summary of Recommendations. We recommend that the DoD Principal Director for Year 2000 meet with Central Design Activities that share noncompliant domains to determine corrective actions required to renovate domains and determine whether noncompliant applications should be classified as mission critical or mission essential. We recommend that the Senior Civilian Official, Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), establish a policy to remove noncompliant applications, executive software, and hardware from shared domains by the start of FY 2000.

Management Comments. The Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) comments concurred with all recommendations. The DoD Principal Director has met with various DoD organizations and senior-level management officials to ensure adequate review of Defense Megacenter domains. Also, the DoD Senior Civilian Official will establish a policy to remove noncompliant products providing that the removal of the noncompliant products does not adversely impact mission support capability.

Evaluation Response. The management comments were responsive. The actions of the DoD Principal Director, in conjunction with the DoD Year 2000 Steering Committee, ensure that senior-level attention will be provided to the domain compliance issue. The Defense Information Systems Agency reported to the DoD Year 2000 Steering Committee on May 25, 1999, that the number of noncompliant domains had been reduced to 79 and a plan was in place to validate those domains by November 1999. We will continue working with the Department to monitor implementation of agreed-upon actions in this crucially important area, where enough risk remains to warrant sustained management emphasis.

Table of Contents

Executive Summary	i
Introduction	
Background	1
Objectives	3
Finding	
Defense Megacenter Domains	4
Appendixes	
A. Evaluation Process	
Scope	8
Methodology	9
Summary of Prior Coverage	9
B. Report Distribution	10
Management Comments	
Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)	13

Background

Congressional Requirement. The National Defense Authorization Act for FY 1999 requires the Inspector General, DoD, to selectively audit information technology and national security systems certified as year 2000 (Y2K) compliant to evaluate the ability of systems to successfully operate during the actual Y2K, including the ability of the systems to access and transmit information from point of origin to point of termination.

DoD Year 2000 Management Strategy. In his role as the DoD Chief Information Officer, the Senior Civilian Official, Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), issued the "DoD Year 2000 Management Plan" (DoD Management Plan) version 2.0, in December 1998. The DoD Management Plan provides the overall DoD strategy and guidance for inventorying, prioritizing, fixing, testing, and implementing compliant systems, and monitoring their progress. The DoD Management Plan describes what each DoD Component must accomplish in each phase of the required five-phase, Y2K management process. The target completion date for implementing all mission-critical systems was December 31, 1998.

Defense Megacenters. The Defense Information Systems Agency (DISA) is the central manager for major portions of the Defense Information Infrastructure. The DISA Western Hemisphere (DISA WESTHEM) executes the DISA mission within the Western Hemisphere Theater. Part of the DISA WESTHEM responsibility is to operate 16 computer-processing organizations, which are called Defense Megacenters.

Computer-Processing Services. The Defense megacenters sell computer-processing services to functional users and are responsible for Y2K compliance of the computer hardware and executive software. Concurrent with the Y2K conversion, (which is a joint and coordinated effort with the Central Design Activities) DISA WESTHEM is also consolidating the mainframe processing into six locations under a 14-month restructuring period that began in April 1998.

Central Design Activities. Central Design Activities (CDAs) develop and maintain application software. Organizationally, the CDAs are part of the Military Departments and Defense agencies. The CDAs are responsible for making the application software Y2K compliant and work within the domains at the Defense Megacenters.

Prior Mainframe Coverage. Inspector General, DoD, Report No. 98-193, "Evaluation of the Defense Megacenters Year 2000 Program," August 25, 1998, identified problems in the reporting, testing, and contingency planning areas.

Reporting. DISA Y2K status reports for executive software were incomplete. The reports showed that the executive software product inventory was 60 percent compliant, but they did not show that the domain compliance was zero percent at that time. Accordingly, DoD was at risk of classifying mission-critical systems on mainframe computers as being Y2K compliant when they were not. The Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) concurred with our recommendation that the DoD Chief Information Officer, in conjunction with the Chief Information Officers of the Military Departments and Defense agencies, direct the CDAs to expedite written agreements with the Defense Megacenters and System Support Offices for the Y2K renovation of domain executive software. At the Steering Committee meeting, July 22, 1998, the Deputy Secretary of Defense directed that written agreements between DISA and domain users be established. The Secretary of Defense memorandum, August 7, 1998, also states that DISA would provide a report to the Office of the Assistant Secretary (Command, Control, Communications, and Intelligence) by October 15, 1998, listing all domain users who failed to sign test agreements with DISA by October 1, 1998. Further, the Director, DISA, agreed that the Defense Megacenters and System Support Offices would do the following:

- establish written agreements with the CDAs and Defense Megacenters to include specific plans and agreements for renovation of domain executive software;
- report complete Y2K status, including the executive software renovations by domain, for inclusion in DISA WESTHEM reports to DISA Headquarters; and
- report the applications that were affected by domain and the status of the coordinated agreements and schedules with the CDAs for inclusion in DISA WESTHEM reports to DISA Headquarters.

Additionally, the Office of the Assistant Secretary (Command, Control, Communications, and Intelligence) and DISA agreed that the Director, DISA, would report domain Y2K compliance status to the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence). The Office of the Assistant Secretary of Defense further agreed that DISA would include items that would identify domains, mission-critical systems, or national security systems that are at high risk of Y2K compliance.

Testing. The DISA did not plan to test the nonstandard executive software, computer hardware, and facility equipment for Y2K compliance. As a result, mission-critical processing may be at risk of date-related failures. The Director, DISA, agreed to selectively test components of the nonstandard executive software, computer hardware, and facility equipment for Y2K compliance. DISA stated that because of time and resource constraints, it would not test all the executive software products, but would meet with customers to decide jointly which products would be tested.

Contingency planning. Although DISA established contingency plans and issued initial guidance to the Defense Megacenters, the guidance needed to

be expanded. Without comprehensive planning, mission-critical systems may not be able to continue operations if Y2K failures occur. The DISA directed the Defense Megacenters to complete risk assessments; plan for contingency coverage of executive software, computer hardware, and facilities equipment; establish contingency planning milestones; and report the status of contingency planning development and contingency plan validation.

Objectives

The objective of this review was to follow up on Inspector General, DoD, Report No. 98-193, "Evaluation of the Defense Megacenters Year 2000 Program," August 25, 1998. Specifically, we evaluated whether the DISA is adequately managing the mainframe domains, in coordination with the Central Design Activities and functional users, to ensure mainframe domain year 2000 compliance. See Appendix A for a discussion of the evaluation scope and methodology.

Defense Megacenter Domains

DISA and the CDAs have made significant progress in identifying and renovating the domains at the Defense Megacenters; however, additional work is needed to lower the risk of year 2000 date-related failures. As of March 31, 1999, DISA had 94 noncompliant domains (80 mainframe and 14 mid-tier). A primary reason for the noncompliant domains was that 71 percent contained one or more noncompliant applications. Also, about 40 percent of the noncompliant domains are shared among Military Departments and Defense agencies. As a result, considerable risk remains to all applications that share noncompliant domains.

Year 2000 Management Guidance

The DoD Management Plan. The DoD Management Plan specifies that DoD will use the Government-wide five-phase management process stipulated by the Office of Management and Budget. The phases and target dates are shown below.

- **Awareness Phase:** Promote Y2K awareness across the entire organization and at all levels of leadership. Target completion date: December 31, 1996.
- **Assessment Phase:** Inventory all systems, identify mission-critical systems, assess each system for risks and issues, develop a strategy to address each risk, prioritize all systems for fixing, and develop contingency plans. Target completion date: June 30, 1997.
- **Renovation Phase:** Replace, repair, or terminate systems to ensure Y2K compliance. Target completion date: June 30, 1998 (mission-critical systems) and September 30, 1998 (all other systems).
- **Validation Phase:** Test systems and certify appropriately for Y2K compliance. DoD requires all mission-critical systems to be certified at the I, IA, IB, 2, 2A, or 2B level. Target completion date: September 30, 1998 (mission-critical systems) and January 31, 1999 (all other systems).
- **Implementation Phase:** Fully deploy renovated and replacement system. Target completion date: December 31, 1998 (mission-critical systems) and March 31, 1999 (all other systems).

Domains

Systems that run on a mainframe computer operate in a logical partition called a domain. The domain concept also includes mid-tier computers. The domain contains applications, executive software, and computer hardware required by

the applications. The executive software includes the operating system and products that provide services such as resource allocation, input and output control, security, and database management.

Domain Renovation

DISA and the CDAs have made significant progress in identifying and renovating the domains at the Defense Megacenters. Table 1 shows that from December 1998 to April 1999, the number of compliant domains increased from 159 to 258. The number of noncompliant domains decreased from 269 to 94. The total number of domains has decreased from 428 to 352.

Table 1. Compliant and Noncompliant Domains

<u>Domains</u>	<u>December 1998</u>	<u>January 1999</u>	<u>March 1999</u>	<u>April 1999</u>
Compliant	159	164	185	258
Noncompliant	269	263	229	94
Total	428	427	414	352

Of 94 noncompliant domains, 80 are mainframe domains (53 percent of the mainframe domains). Forty percent of the 94 noncompliant domains are shared among Military Departments and Defense Agencies.

Renovation and Validation Target Completion Dates

Table 2 shows that the validation schedule for noncompliant domains has slipped.

Table 2. Changing Validation Plans

<u>Domains Scheduled for Validation</u>	<u>December1998</u>	<u>January 1999</u>	<u>March 1999</u>	<u>April 1999</u>
Post March 31, 1999	39	35	56	94

The remaining 94 noncompliant domains missed the renovation and validation target dates and also the implementation date of March 31, 1999, to complete the phases delineated in the DoD Management Plan.

Table 3 illustrates the current plan for validating the remaining 94 noncompliant domains.

Table 3. Domain Validation Plan

<u>Month to be Completed in 1999</u>	<u>Domains</u>
April	25
May	27
June	15
July	2
August	4
September	12
October	1
November	6
December	2
Total	94

Reasons for Domain Renovation

Table 4 shows why the domains remain noncompliant. One or more noncompliant applications were the reason for 71 percent of the noncompliant domains.

Table 4. Reasons for Domain Renovation After March 31, 1999

	<u>Domains</u>
Noncompliant Executive Software	20
Noncompliant Computer Hardware	7
Noncompliant Application	67
Total	94

If an application, an executive software product, or a required computer hardware item fails, the domain can also fail. All applications that share domains with noncompliant applications, executive software, and computer hardware remain at high risk of failure.

Recommendations, Management Comments and Evaluation Response

1. We recommend that the DoD Principal Director Year 2000:
 - a. Meet with the Central Design Activities for the applications that share a noncompliant domain to review the status and necessary actions to renovate the domains.

-
- a. **Meet with the Central Design Activities for the applications that share a noncompliant domain to review the status and necessary actions to renovate the domains.**
 - b. **Determine whether to classify noncompliant applications, that share domains with mission-critical applications, as mission critical or mission essential.**
 2. **We recommend that the DoD Senior Civilian Official, Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), establish a policy to remove, by the start of FY 2000, noncompliant applications, executive software, and hardware from any mainframe domain shared by a compliant application, even if the compliant application belongs to the same Military Department or Defense agency.**

Management Comments

The Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) stated that the DoD Principal Director for Y2K has taken action to ensure adequate review of the status of the Defense Megacenter domains. The DoD Principal Director meets regularly in various forums, including the DoD Year 2000 Steering Committee, to discuss issues on domain compliance. Additionally, policy instructions have been issued to the Military Departments and the Defense Agencies regarding reporting procedures for domain data. Based on the senior-level management meetings, the Senior Civilian Official is aware of the domain status issue and plans to establish a policy to remove noncompliant products from shared domains as long as there is no adverse impact to mission support capability.

Evaluation Response

We consider the management comments, in conjunction with ongoing senior level reviews of domain compliance, to be responsive to the intent of the recommendations. Compliance of the Megacenter domains has been an agenda item at the DoD Year 2000 Steering Committee meetings, chaired by the Deputy Secretary of Defense. Senior management attention on the Defense Megacenters should allow adequate resolution of issues pertaining to domain compliance. At the DoD Year 2000 Steering Committee meeting on May 25, 1999, DISA reported continued progress. The number of noncompliant domains had been reduced to 79 and a plan was in place to achieve complete compliance by November 1999. We will continue working with the Department to monitor implementation of the agreed-upon actions in this crucial area, where sufficient risk remains to warrant special management attention.

Appendix A. Evaluation Process

This report is one in a series being issued by the Inspector General, DoD, in accordance with an informal partnership with the Chief Information Officer, DoD, to monitor DoD efforts to address the Y2K computing challenge. For a listing of audit projects addressing the issue, see the Y2K web page on the IGnet at <http://www.ignet.gov>.

Scope

Review of the Megacenter Domains. We selected a judgmental sample of domains at each Defense Megacenter to determine their Y2K status. Our scope was limited to determining status of recommendations for Inspector General, DoD, Report No. 98-193, "Evaluation of the Defense Megacenters Year 2000 Program," August 25, 1998. We conducted this technical assessment in accordance with standards implemented by the Inspector General, DoD.

DoD-Wide Corporate-Level Government Performance and Results Act Goals. In response to the Government Performance Results Act, the Department of Defense has established 6 DoD-wide corporate level performance objectives and 14 goals for meeting the objectives. This report pertains to achievement of the following objective and goal.

Objective: Prepare now for an uncertain future. **Goal:** Pursue a focused modernization effort that maintains U.S. qualitative superiority in key war fighting capabilities. (DoD-3)

DoD Functional Area Reform Goals. Most major DoD functional areas have also established performance improvement reform objectives and goals. This report pertains to achievement of the following functional area objectives and goals.

Information Technology Management Functional Area.

- **Objective:** Become a mission partner.
Goal: Serve mission information users as customers. (ITM-1.2)
- **Objective:** Provide services that satisfy customer information needs.
Goal: Modernize and integrate Defense information infrastructure. (ITM-2.2)
- **Objective:** Provide services that satisfy customer information needs.
Goal: Upgrade technology base. (ITM-2.3)

General Accounting Office High-Risk Area. In its identification of risk areas, the General Accounting Office has specifically designated risk in resolution of

the Y2K problem as high. This report provides coverage of that problem and of the overall Information Management and Technology high-risk area.

Methodology

Audit Type, Dates, and Standards. We performed this evaluation from February through April 1999. This review was limited to actions taken in response to recommendations in Inspector General, DoD, Report No. 98-193, "Evaluation of the Defense Megacenters Year 2000 Program," August 25, 1998. We conducted this technical assessment in accordance with standards implemented by the Inspector General, DoD.

Contacts During the Audit. We visited or contacted individuals and organizations within DoD. Further details are available upon request.

Management Control Program. We did not review the management control program related to the overall audit objective because DoD recognized the Y2K issue as a material management control weakness area in the FY 1998 Annual Statement of Assurance.

Summary of Prior Coverage

The General Accounting Office and the Inspector General, DoD, have conducted multiple reviews related to Y2K issues. General Accounting Office reports can be accessed over the Internet at <http://www.gao.gov>. Inspector General, DoD, reports can be accessed at <http://www.dodig.osd.mil>.

Appendix B. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition and Technology
Director, Defense Logistics Studies Information Exchange
Under Secretary of Defense (Comptroller)
Deputy Chief Financial Officer
Deputy Comptroller (Program/Budget)
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
Deputy Assistant Secretary of Defense (Command, Control, Communications, and Intelligence, Surveillance, Reconnaissance, and Space Systems)
Deputy Chief Information Officer and Deputy Assistant Secretary of Defense (Chief Information Officer Policy and Implementation)
Principal Director for Year 2000
Assistant Secretary of Defense (Public Affairs)

Department of the Army

Assistant Secretary of the Army (Financial Management and Comptroller)
Chief Information Officer, Department of the Army
Inspector General, Department of the Army
Auditor General, Department of the Army

Department of the Navy

Assistant Secretary of the Navy (Financial Management and Comptroller)
Chief Information Officer, Department of the Navy
Inspector General, Department of the Navy
Auditor General, Department of the Navy
Inspector General, Marine Corps

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Chief Information Officer, Department of the Air Force
Inspector General, Department of the Air Force
Auditor General, Department of the Air Force

Defense Organizations

Director, Defense Contract Audit Agency
Director, Defense Information Systems Agency
 Inspector General, Defense Information Systems Agency
 Chief Information Officer, Defense Information Systems Agency
 United Kingdom Liaison Officer, Defense Information Systems Agency
Director, Defense Logistics Agency
Director, National Security Agency
 Inspector General, National Security Agency
Inspector General, Defense Intelligence Agency
Inspector General, National Imagery and Mapping Agency
Inspector General, National Reconnaissance Office

Non-Defense Federal Organizations and Individuals

Chief Information Officer, General Services Administration
Office of Management and Budget
 Office of Information and Regulatory Affairs
General Accounting Office
 National Security and International Affairs Division
 Technical Information Center
 Director, Defense Information and Financial Management Systems, Accounting
 and Information Management Division, General Accounting Office

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
Senate Special Committee on the Year 2000 Technology Problem
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Reform
House Subcommittee on Government Management, Information, and Technology,
 Committee on Government Reform
House Subcommittee on National Security, Veterans Affairs, and International
 Relations, Committee on Government Reform
House Subcommittee on Technology, Committee on Science

Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) Comments



COMMAND, CONTROL,
COMMUNICATIONS, AND
INTELLIGENCE

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

May 21, 1999

MEMORANDUM FOR DIRECTOR, ACQUISITION MANAGEMENT
DIRECTORATE, INSPECTOR GENERAL, DOD

SUBJECT: Defense Information Systems Agency Management of Mainframes
(Project No. 9AS-0092)

The Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) (OASD(C3I)) has reviewed the Draft Audit Report on the Defense Information Systems Agency Management of Mainframes, dated April 26, 1999. We have determined that the recommendations presented on Page 7, Paragraph 1a & b to be performed by the DoD Principal Director, Year 2000 (Y2K) will comply with the recommendations. The Y2K Office has taken several steps to ensure adequate review of the status and necessary actions to remediate applications that share non-compliant domains. Therefore, we recommend that your recommendations be modified based on the following information:

- a. DoD Principal Director for Y2K will continue regular engagement with the Military Services and Agencies' Chief Information Officer at DoD Steering Committee Meetings, Joint Staff Synchronization Meetings, Defense Information Systems Agency Director Meetings and Y2K Services and members of the Senior Executive Services to include discussion of renovation of non-compliant applications that share DISA domains. It is anticipated that the information discussed at these meeting will be promulgated to the Central Design Activities.
- b. The DoD Principal Director for Y2K attends all quarterly DISA Partnership Review of Domains meetings hosted by the DISA Director, LTG David Kelley.
- c. The Principal Director for Y2K is holding DISA domain meetings immediately after all CINC meetings to ensure adequate review of the status of domains and facilitate any necessary actions to remediate applications that share non-compliant domains.
- d. The DoD Principal Director for Y2K ensures DISA domain data is reported to the Y2K Steering Committee, chaired by the Deputy Secretary of Defense.
- e. The DoD Principal Director for Y2K has issued policy instructions to the Military Departments and Defense Agencies that will permit the capture of all applications that cause domains to be non-compliant after June 30, 1999, regardless of their




mission criticality. To facilitate proper reporting and monitoring, these applications will be entered into the OSD Y2K database by May 14, 1999, to ensure the capability of generating appropriate reports for the Deputy Secretary of Defense and Congress.

We will comply with your final recommendation presented on Page 7, Paragraph 2 to be performed by the DoD Senior Civilian Official, Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence). However, we recommend that your recommendation be modified based on the following information:

The OASD(C3I) will establish a policy to remove, by the start of FY 2000 (October 1, 1999), non-compliant applications, executive software, and hardware which share domains with compliant applications, provided said removal will not adversely impact the mission support capability of the Military Departments or Defense Agencies. In the event that an application is removed from a domain, DISA will ensure that any non-compliant hardware or executive software that has been retained on a domain to support that application will be removed if not required by any other application. DISA will not remove non-compliant executive software for which a customer has received a waiver from OASD(C3I). Determination of application removal will be made by the DoD Principal Director Year 2000. OASD(C3I) will work with the Military Departments and Defense Agencies to identify impact (cost and operational) of the policy. OASD(C3I) will also determine whether to apply the policy to other mission critical systems not supported through the DISA, Defense Megacenters.

We will continue our close coordination with the Military Services and Defense Agencies to ensure there is improvement in the area of domain reporting and tracking.

My point of contact for additional information is Mr. Walter Benesch, telephone: (703) 602-0980 ext 129 or Mr. Willie Moss, telephone: (703) 602-0980 ext. 105.


Marvin J. Langston
Deputy Assistant Secretary of Defense
(Deputy CIO & Year 2000)

Evaluation Team Members

The Acquisition Management Directorate, Office of the Assistant Inspector General for Auditing, DoD, produced this report. Personnel of the Office of the Inspector General, DoD, who contributed to the report, are listed below.

Thomas F. Gimble
Patricia A. Brannin
Kenneth H. Stavenjord
Mary Lu Ugone
Thomas Bartoszek
Dan B. Convis
Dianna J. Pearson
Hugh G. Cherry
JoAnn Henderson
Julius Hoffman
Thelma Jackson
Robin McCoy
Herbert Braun
Cristina Maria H. Giusti

INTERNET DOCUMENT INFORMATION FORM

A . Report Title: Defense Information Systems Agency Management of MainFrames

B. DATE Report Downloaded From the Internet: 08/06/99

C. Report's Point of Contact: (Name, Organization, Address, Office Symbol, & Ph #): OAIG-AUD (ATTN: AFTS Audit Suggestions)
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-2884

D. Currently Applicable Classification Level: Unclassified

E. Distribution Statement A: Approved for Public Release

F. The foregoing information was compiled and provided by:
DTIC-OCA, Initials: __VM__ Preparation Date 08/06/99

The foregoing information should exactly correspond to the Title, Report Number, and the Date on the accompanying report document. If there are mismatches, or other questions, contact the above OCA Representative for resolution.